EXHIBIT N

Information Security Policy

Information Security

Effective Date:

07/08/2020

Table of Contents

Impacted Teams:	*All Personnel*	
For Questions Email:	*ISO@loanDepot.com*	
Related Material:	*Data Classification Policy*	*Data Handling Procedure*

1. Purpose

This policy has been established to set the ground rules under which the Company operates and safeguards its data and information systems to both reduce risk and minimize the effect of potential incidents. Additionally, this policy sets the standards for safeguarding Company Information (CI) from misuse and unauthorized disclosure. The policy provides information on the prescribed measures used to establish and enforce the Information Security program at loanDepot.

For purposes of this policy, the "Company" refers to loanDepot (LD) and its subsidiaries.

1.1. Information Security Program Framework

The information security program provides the framework for:

- Creating an Information Security Management System (ISMS) in accordance with ISO 27001.
- Protecting the confidentiality, integrity, and availability of CI and information systems.
- Protecting the Company, its employees, and its clients from illicit use of the Company's information systems and data.
- Ensuring the effectiveness of security controls over data and information systems that support the Company's operations.
- Providing for development, review, and maintenance of minimum-security controls required to protect the Company's data and information systems.

The security program is driven by many factors, with risk being the key factor. This policy and its related procedures are necessary to mitigate the risks in daily operations, and to ensure users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent practices for managing the security of information across the company helps to maintain compliance with current and future legal obligations in protecting the confidentiality, integrity and availability of the CI.

1.2. Policy Statement

The Company is committed to protecting its employees, partners, clients, customers and the Company from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every user who interacts with data and information systems. Therefore, it is the responsibility of every user to know this policy and to conduct their activities accordingly.

- Protecting CI and the systems that collect, process, and maintain this information is of critical importance.
- The security of information systems must include controls and safeguards to offset possible threats and vulnerabilities, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data.
- Security measures must be taken to safeguard against unauthorized access to, alteration of, or disclosure of data and information systems. This also includes safeguarding against accidental loss or destruction.

The Company reserves the right to revoke, change, or supplement this policy at any time without prior notice. Such changes shall be effective immediately upon approval by management, unless otherwise stated.

2. Scope

This policy applies to all CI, information systems, activities, and assets owned, leased, controlled, or used by Company employees, its agents, temporary employees, contractors, or other business partners on behalf of the Company.

For purposes of this policy all employees, temporary employees, contractors, sub-contractors, and their respective facilities supporting Company business operations, wherever CI is stored or processed, including any third party contracted by the Company to handle, process, transmit, store, or dispose of CI, will be defined and combined as Company "personnel".

Any persons that have access to CI are hereafter referenced as "Users" throughout this document. Some sections of this policy are explicitly stated for persons with a specific job function (e.g., a system administrator, asset custodian, or data owner); otherwise, all Company personnel shall comply with this policy.

This policy does not supersede any other applicable law or regulation, higher-level company directive, or existing labor management agreement in effect as of the effective date of this policy.

3. Definitions

Refer to Addendum 11.1 for a Glossary of Information Security Terms and Concepts.

4. Roles & Responsibilities

All company personnel are responsible for safe handling and protecting business information assets. This includes safeguarding and monitoring against unauthorized disclosure, modification, and destruction.

The following table provides the different roles and responsibilities for Information Security:

Role	Responsibility
Chief Information Security Officer (CISO)	Overseeing the development and execution of the Company's Information Security and Privacy programs and for ensuring that they align with legislative requirements and business goals. The CISO is also responsible for chairing the Information Security Steering Committee.
Chief Privacy Officer (CPO)	Establishing and directing all phases of the Privacy program to ensure that it aligns with legislative requirements and business goals.
Vice President Cyber Security	Directing all phases of the Information Security program and managing the overall information security posture consistent with the Company's risk appetite.
Asset Custodian	Assuring that assets are properly maintained, used for the purposes intended, and information regarding equipment is properly documented. Asset Custodian is a person or entity.
Data Owner	Making sure assets are secure while they are being developed, produced, maintained, and used. The Data Owner is a person or entity that has been given formal responsibility for the security of an asset, asset category, or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense.

Information Security Management	Supporting and maintaining the Information Security Policy and monitoring the effectiveness of, and the level of compliance with, this policy. Ensuring personnel are informed and updated regarding their security responsibilities, and that personnel under their supervision are motivated to support the security policies of the Company.
Users	Protecting and handling information in accordance with the *Data Handling Procedure*. Users are the individuals, groups, or company authorized by the data owners to access information.
Third Parties	Securing any business information assets to which they have access and ensuring no further dissemination of the information takes place to any other third party without prior written consent from the company. Third Parties are customers, partners, vendors, contractors, dealers, and associates, who do business with the Company.

5. Policy Detail

Company expectations are outlined in this section for the development, implementation, assessment, authorization, and monitoring of the Information Security program.

This policy incorporates requirements to protect the confidentiality, integrity, availability, and privacy of Company data and information systems, regardless of how data are created, distributed, or stored. Information security controls shall be tailored so that cost-effective solutions can be applied commensurate with the risk and sensitivity of the data and information system, in accordance with all legal obligations.

5.1. Information Security Management System (ISMS)

The objective of ISMS is to provide management direction and support for information security in accordance with business requirements, best practices, and relevant laws and regulations.

An ISMS focuses on Information Security management and related risks. The governing principle behind the Company's ISMS is it must remain effective and efficient long-term, adapting to changes within the Company and external environments.

In accordance with ISO/IEC 27001, the Company's ISMS shall incorporate the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle:

Approach	Description
Plan	This phase involves designing the ISMS, assessing related threats, vulnerabilities and risks, and selecting appropriate controls.
Do	This phase involves implementing and operating the appropriate security controls.
Check	This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
Act	This phase involves making changes, where necessary, to bring the ISMS back to optimal performance.

5.2. Organization of Information Security

This management framework is intended to initiate and control the implementation and operation of Information Security within the Company. This section provides the requirements for establishing,

implementing, maintaining, and continually improving the Company ISMS. These requirements consider the Company issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of the ISMS.

5.3. Information Security's Role and Responsibilities

Information security strategic initiatives are coordinated through the Information Security Steering Committee, which shall assist the CISO with the strategic development and implementation of the Information Security Program.

All Information Security roles and responsibilities shall be clearly defined and allocated for all Information Security staff by collaboratively working with Human Resources (HR).

5.3.1. During Employment

The Company shall ensure that personnel understand and fulfill their information security responsibilities.

Company personnel must accept and acknowledge their information security responsibilities as part of the on-boarding process and complete the information Security training within 60 days.

5.3.2. Segregation of Duties

Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Company's assets. Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of Company assets. The Company shall ensure the following:

No single person has the ability to access, modify, or use critical assets without authorization (e.g., the initiation of an event should be separated from its authorization). The possibility of collusion should be considered in designing the controls.

User account creation requests and access entitlement request must not be self-approved by the requestor.

Business managers or their delegates cannot review or approve their own access entitlements.

Information system developer privileges to change hardware, software, and firmware components and system information within a production/operational environment are prohibited.

Where segregation of duties is difficult to achieve, the Company will use other controls such as monitoring of activities, audit trails and management supervision to ensure risk is managed.

5.3.3. Contacts with Authorities

As part of the Company's information security response capability, procedures must be in place that specify when and by whom authorities (e.g., law enforcement, regulatory bodies, and supervisory authorities) must be contacted and how information security incidents must be reported.

5.3.4. Information Security in Project Management

Information security shall be integrated into the organization's project management methodology to ensure information security risks are identified and addressed as part of a project. The intent is to identify potential threats, vulnerabilities risks, and concerns at the early stages of project planning and to manage them throughout the lifecycle.

5.3.5. Information Security Awareness, Education and Training

All Company personnel must receive appropriate awareness education, training, and regular updates in Company policies and procedures, as relevant for their job function. The HR and/or Training department shall ensure initial information security training is provided to personnel upon hire, and the Information

Security Department (ISD) is required to provide training, at least annually, thereafter. The Information Security team, in collaboration with the Training Department, shall implement a formal security awareness program to ensure all personnel are aware of important and evolving information security and privacy topics.

5.4. Asset Management

The purpose of this section is to ensure that assets and data are properly inventoried and measures are implemented to protect the Company's data from unauthorized disclosure, regardless if it is being transmitted or stored.

5.4.1. Inventory of Assets

An accurate inventory of all Company IT assets must be maintained on an ongoing basis.

Inventory Type	Responsibility
Hardware Inventory	The Company shall develop, document, and maintain an inventory of hardware assets that: • Accurately reflects the current information system. • Is at the level of granularity deemed necessary for tracking and reporting. • Is available for review and audit.
Application Inventory	The company must maintain a current inventory of applications (including web-based applications) which must be reviewed for accuracy and completeness. IT management must review the inventory for accuracy at least annually.

5.4.1.1. Network Diagrams

Asset custodians and data owners must:

- Verify that a current network diagram exists for their environment(s).
- Maintain a current diagram that shows all CI data flows across systems and networks.
- Documents all connections, including any wireless networks and hosted services.

5.5. Access Control

Access controls are required for all Company information systems in accordance with the appropriate level of risk. Managers are accountable for the access rights of the users under their supervision. All access controls must support the concept of "least privilege" through limiting access to information systems and data to authorized users only. In this regard, Users will be given only those privileges and access rights which are essential to perform their intended and required functions for and responsibilities to the Company.

5.5.1. Access to Company Information Systems

The Company shall limit the access to information systems and CI to only those individuals whose job requires such access.

Access limitations include the following:

a) Defining access needs for each role, including:

- System components and Company information resources that each role needs to access for their job function; and
- Level of privilege required (e.g., user, management, asset custodians, etc.) for accessing Company information resources;

b) Restricting access to user IDs to the least privileges and time necessary to perform job responsibilities;

c) Assigning access based on individual user's job classification and function; and

d) Requiring documented approval by authorized parties specifying required privileges.

5.5.2. Access to Networks and Network Services

Users will be provided with access to the network and network services that they have been specifically authorized to use.

5.5.2.1. Least Privilege

The Company shall employ the concept of least privilege, allowing only authorized accesses for users and processes which are necessary to accomplish assigned tasks in accordance with Company business functions. Access will be granted only for the minimum:

a) Levels of permissions necessary to perform the job function; and

b) Time required performing the job function.

5.5.2.2. Mobile Devices and Remote Access

The purpose of this section is to manage the threats, vulnerabilities, and risks introduced by using mobile devices. It also specifies the requirements that shall be implemented to protect information accessed, processed or stored at teleworking sites.

5.5.2.2.1. Company Owned Mobile Device Management

When using mobile devices, special care should be taken to ensure that Company Information is not compromised. The Company shall ensure the following requirements are met for Company-owned mobile devices:

Topic	Requirements
Loss / Theft	Mobile devices are required to be physically protected against theft especially when left in a car and other forms of transport (e.g., hotel rooms, conference centers and meeting places). Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away to secure the devices. Users must notify Company management when a mobile device is lost or stolen within twelve (12) hours. Users will alert management of the circumstances surrounding the loss and the data contained on the mobile device.
Passwords	A password or PIN with a minimum of six (6) characters, facial recognition, or fingerprint must be used to log onto the device.
Lockout	The mobile device must be set to delete all data or lock internally after five (5) unsuccessful attempts to enter a password or PIN.

Encryption	The mobile device must be encrypted.
Encrypted Data Backups	All data on mobile devices must be encrypted, when backed up.
Anti-malware	Antimalware software must be installed on mobile devices that are capable of running such software
Updates	Mobile device and installed applications must be kept updated with the latest software releases.
Rooting	Users must not: • Circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., “jailbreaking”). • Tamper with the mobile device by using unauthorized software, hardware, or other methods.
Wireless	Users are required to ensure Company information security requirements are maintained when connecting the mobile device to other devices and networks: • Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices. • Users may use only secure (e.g., WPA2) Wi-Fi networks known to be trustworthy. • When using mobile devices in public locations, users should be aware of potential shoulder surfing. To avoid individuals looking over your shoulder, use a privacy screen or sit with your back to the wall. The Company is not responsible for overages or data plans for cellular usage.
Remote Purging	The Company shall provide the capability to remotely purge company information from mobile devices.

5.5.2.2.2. Employee Owned Devices

Employee owned devices must connect to the Guest Wi-Fi network to ensure that Company Information is not compromised. The Employee shall ensure the following requirements are met for employee owned mobile devices.

Topic	Requirements
Loss / Theft	Mobile devices should be physically protected against theft especially when left in a car and other forms of transport (e.g., hotel rooms, conference centers and meeting places). Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away to secure the devices. Users must notify Company management when a mobile device is lost or stolen within twelve (12) hours. Users will alert management of the

	circumstances surrounding the loss and the data contained on the mobile device.
Passwords	A password or PIN with a minimum of six (6) characters, facial recognition, or fingerprint must be used to log onto the device.
Encryption	The mobile device must be encrypted.
Encrypted Data Backups	All data on mobile devices must be encrypted, when backed up.
Updates	Mobile device and installed applications must be kept updated with the latest software releases.
Rooting	Users must not: • Circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., “jailbreaking”). • Tamper with the mobile device by using unauthorized software, hardware, or other methods.
Wireless	Users are required to ensure Company information security requirements are maintained when connecting the mobile device to other devices and networks: • Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices. • Users may use only secure (e.g., WPA2) Wi-Fi networks known to be trustworthy. • When using mobile devices in public locations, users should be aware of potential shoulder surfing. To avoid individuals looking over your shoulder, use a privacy screen or sit with your back to the wall. The Company is not responsible for overages or data plans for cellular usage.
Remote Purging	The Company shall provide the capability to remotely purge company information from mobile devices.

5.5.2.2.3. Teleworking

Teleworkers shall only access company resources from company-issued or approved personal devices.

Accessing company resource through anonymizing services such as personal VPNs is strictly prohibited.

Supporting security measures must be implemented to protect information accessed, processed or stored at teleworking sites.

Access Type	Requirements
Remote Access	The Company’s Information Security personnel are responsible for: • Documenting allowed methods of remote access to the information system.

	• Establishing usage restrictions and implementation guidance for each allowed remote access method. • Monitoring for unauthorized remote access to information systems. • Authorizing remote access to information systems prior to connection. • Enforcing requirements for remote connections to information systems. • Using cryptography to protect the confidentiality and integrity of remote access sessions. • Immediately deactivating vendor and business partner remote access when it is no longer needed.

5.5.3. User Access Management

The Company shall ensure authorized user access and prevent unauthorized access to systems and services. A formal user provisioning and de-provisioning process must be implemented to enable assignment of access rights.

5.5.3.1. Termination or Change of Employment Responsibilities

The objective of this section is to protect LD's interests as part of the process of changing or terminating employment.

5.5.3.1.1. Termination and Removal of Access Rights

Management, upon termination of individual employment, is required to complete the appropriate off-boarding process within 24 hours.

- Physical building access
- Active Directory Account
- Remote access rights must be disabled for all terminated personnel
- Access to critical applications that can access CI must be disabled.
- Access to all other applications that can access CI must be disabled within 30 days of termination.

Upon termination of an individual deemed to be a "high risk" to the Company, the process of removing the individual's access to CI, data, and information systems must be expedited and Human Resources (HR) must immediately notify the Company's Information Security personnel to revoke the user's IDs, privileges, and authorizations.

Management is responsible for the following:

Action	Responsibility
User Transfer	For submitting an appropriate user access form (UAF) when an employee's role significantly changes, such as relocating into a new business segment, or changing manager and location. Management must note if current access rights must be retained or revoked when initiating the UAF and shall: • Review the logical and physical access authorizations to information systems/facilities when users are reassigned or transferred to other positions within the Company.

	• Initiate Company-defined transfer or reassignment actions within seven (7) days following the formal transfer action.
Return of Assets	For ensuring that LD personnel return Company assets in their possession at the termination of their employment or contract in accordance with the Section 5.3 (Acceptable Use) of this policy and local laws and regulations.

5.5.3.2. User ID Management

The Company shall ensure proper user identification management on all information systems.

Asset custodians must assign all users unique user identification (ID before allowing them to access information systems). User identification controls will include the following:

- Controlling addition, deletion, and modification of user IDs, credentials, and other identifier objects;
- Disabling/revoking access to terminated users within two business days of notification of employment status change;
- Removing or disabling inactive user accounts that have been inactive for ninety (90) days or more;
- Managing user accounts assigned to vendors that are used to access, support, or maintain system components via remote access;
- Limiting repeated access attempts be locked out after not more than five (5) invalid logon attempts;
- Setting lockout durations to a minimum of thirty (30) minutes or until an administrator enables the user ID; and
- Require users to re-authenticate if a session has been idle for more than ten (10) minutes to re-activate the terminal or session.

5.5.3.3. Account Management [by system or application]

The Company must manage information system accounts.

5.5.3.4. User Access Provisioning

A formal user access provisioning process must be implemented to assign or revoke access rights for all user types to all systems and services. Authentication mechanisms must be established to verify user legitimacy.

a) Use strong cryptography to render all authentication credentials unreadable during transmission and storage;

b) Verify user identity before modifying any authentication credential that includes, but is not limited to:

   - Performing password resets;
   - Provisioning new tokens; or
   - Generating new keys;
   - Require complex passwords/phrases (see *Section 5.5.6 Password Management* for more information)

- Set passwords/phrases for first-time use and upon reset to a unique value for each user and change immediately after the first use.

5.5.3.5. Role-Based Access Control (RBAC)

The Company shall establish Role Based Access Control (RBAC) access enforcement that:

a) Assigns privileges to individuals based on job classification and function; and

b) Restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

5.5.4. Database Access

Asset custodians must restrict all access to any database containing CI (including access by applications, administrators, and all other users), as follows:

a) All user access to, user queries of, and user actions on databases must be through programmatic methods.

b) Direct access to query functionality may only be given on a restricted basis as determined by the *Data Classification Policy.*

c) Application IDs for database applications may only be used by the applications (not by individual users or other non-application processes).

5.5.5. Secure Log-on Procedures

5.5.5.1. Trusted Communications Path

Information systems must establish a trusted communications path between the user and the security functions of the system.

Where technically feasible, information systems must authenticate with Active Directory (AD).

5.5.5.2. Device-to-Device Identification & Authentication

Information systems must uniquely identify and authenticate devices before establishing a connection.

The Company shall use Active Directory (AD) to authenticate devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

5.5.6. Password Management

The Company must manage information system accounts (authenticators) for users and devices by maintaining the following:

User and Service Account Passwords:

Component	Requirements
Length	• User Accounts: Minimum of ten (10) characters. • Service Accounts: Minimum of fifteen (15) characters.
Reuse	• Twenty-Four (24) - Users cannot use any of the last 24 passwords he or she has used.
Life	• Maximum: Ninety (90) days

Complexity	• Passwords are not a derivative of the user ID. • Passwords have at least one (1) lower alpha, one (1) upper alpha, one (1) number, and one (1) special character, where applicable.

5.5.6.1. Password Protection

Company personnel must ensure that the passwords are kept confidential and must not be shared, written down, or stored in clear text. Users are not authorized to use the same password for their Company accounts as for other non-Company access (e.g., personal ISP account, online banking, benefits, etc.).

a) Users must not use the same password for various Company access needs and are recommended to have unique passwords for each account they access.

b) All passwords are to be treated as Restricted Company Information.

c) Passwords must not be written down and exposed.

5.5.6.1.1. Compromise

If an account or password is suspected to have been compromised, users must report the incident to management and change all passwords immediately.

5.5.6.2. Vendor-Supplied Defaults

The Company must change vendor-supplied defaults before installing a system on the network.

Asset custodians and data owners must change vendor-supplied defaults before installing a system on the network, including but not limited to:

a) Passwords;

b) Encryption keys;

c) Simple Network Management Protocol (SNMP) strings; and

d) Removing unnecessary, default accounts.

5.5.7. Access Control to Program Source Code

5.5.7.1. Source Code

The Company shall retain the source code for custom-developed applications when permissible. Developers are required to provide Asset owners with source code for custom-developed applications.

5.5.7.2. Library Privileges

The Company must limit privileges to change software resident within software libraries. Data owners are required to limit privileges to change software archived within software libraries.

5.6. Cryptography

The purpose of this section is to ensure the confidentiality of the Company's data through implementing appropriate cryptographic technologies that protect information systems and data.

5.6.1. Cryptographic Controls

The Company shall ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information.

5.6.1.1. Use of Cryptography

Use of encryption must be implemented using cryptographic modules that comply with applicable local, state, and federal laws, as well as non-regulatory requirements that the Company is contractually bound to address.

Asset custodians and data owners must ensure information systems storing, processing, or transmitting CI:

a) Employ cryptographic mechanisms;

b) Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard CI during transmission over public or private networks, in accordance with the Company's *Data Handling Procedure* and the *Data Classification Policy*;

c) Verify that the strongest practical encryption strength is implemented for the encryption methodology in use; and

d) Verify that the protocol is implemented to use only secure configurations.

5.6.1.2. Transmission Confidentiality

The Company shall protect the confidentiality of transmitted information. Asset custodians and data owners must employ cryptographic mechanisms to prevent unauthorized disclosure of sensitive information during transmission in accordance with the Company's *Data Handling Procedure* and the *Data Classification Policy*.

5.6.1.3. Wireless Access Authentication & Encryption

Information systems must protect wireless access using authentication and encryption. The Company must ensure wireless networks use industry best practices to implement strong encryption for authentication and transmission, commensurate with the sensitivity of the data being transmitted.

5.6.1.4. Encrypting Data at Rest

Information systems must protect the confidentiality and integrity of CI at rest. Asset custodians and data owners must protect CI by:

a) Employing cryptographic mechanisms to prevent unauthorized disclosure and modification of CI at rest unless otherwise protected by alternative physical measures. Refer to the Company's *Data Handling Procedure* and the *Data Classification Policy* for additional details.

- If disk encryption is used (rather than file-level or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (i.e. by not using local user account databases); and
- Not tying user accounts to decryption keys.

5.6.1.5. Non-Console Administrative Access

The Company shall encrypt all non-console administrative access using strong cryptography. Information Security must develop configuration standards to ensure all non-console administrative access is encrypting using strong cryptography using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

5.6.1.6. Key Management

5.6.1.6.1. Key Management Strategy

The Company shall implement a key management strategy to protect keys used to secure PII against disclosure and misuse. Asset custodians must implement administrative and technical measures to protect keys used to secure PII against disclosure and misuse, including the following:

a) Cryptographic key access shall be restricted to the fewest number of custodians necessary;

b) Cryptographic key access shall be securely stored at all times using one of the following methods:

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key; or
- Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device); and

c) Cryptographic keys must be securely stored in the fewest possible locations and forms.

5.6.1.6.2. Key Management Processes

The Company shall document and implement key management processes and procedures for cryptographic keys used for encryption of PII. Asset custodians must document and implement key management processes and procedures for cryptographic keys used for encryption of PII that includes the following:

a) Procedures for the generation, distribution, and storage of keys:

- Generation of strong cryptographic keys;
- Prevention of unauthorized substitution of cryptographic keys;
- Distribution of cryptographic keys using secure methods; and
- Secure storage of cryptographic keys.

b) Changing cryptographic keys that have reached the end of their crypto period:

- After a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key;
- As defined by the associated application vendor or key owner; or
- Based on industry best practices and guidelines.

c) Retiring or replacing keys when the integrity of the key has been weakened or the keys are suspected of being compromised:

- Retiring or replacing may be performed by archiving, destruction, and/or revocation of keys.
- Keys must be considered compromised by departure of an employee with knowledge of a clear-text key.

5.7. Physical and Environmental Security

The purpose of this section is to minimize risk to the Company information systems and data by addressing applicable physical security and environmental concerns.

5.7.1. Physical Security Perimeter

Security perimeters must be defined and used to protect areas that contain both sensitive or critical information and information systems.

5.7.1.1. Physical Access Authorizations

The Company shall:

a) Develop and keep current, a list of users with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

b) Maintain the access list to include only those users who currently require access.

5.7.1.2. Role-Based Physical Access

The Company shall authorize physical access to the facility where the information system resides, based on the position or role of a user.

5.7.1.3. Physical Access Control

The Company shall:

a) Control entry to the facility containing the information system using physical access devices and/or safeguards;

b) Secure keys, combinations, and other physical access devices; and

c) Change combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

5.7.1.4. Physical Access Logs

The physical access control system must generate a log entry for each access. The Company shall configure access control systems to log the following information:

a) Physical location of the access;

b) Direction of access, if possible (e.g., ingress or egress);

c) Identity of the person accessing the location; and

d) Indication of success or failure.

5.7.1.5. Access Control for Transmission Medium

The Company shall control physical access to information system distribution and transmission lines within facilities and limit access to transmission medium only to authorized personnel.

5.7.2. Security of Company Equipment and Assets Off-Premises

Security must be applied to off-site assets taking into account the different risks of working outside the Company's premises.

5.7.2.1. Media Distribution

The Company's asset custodians and data owners must maintain strict control over the internal or external distribution of media, including the following:

a) Classifying media in accordance with the *Data Classification Policy* and *Data Handling Procedure* so the sensitivity of the data can be determined;

b) Sending sensitive media by secured courier or other delivery method that can be accurately tracked; and

c) Ensuring prior management approval for any and all media that is moved from a secured area (including when media is distributed to individuals).

5.7.3. Secure Disposal or Re-use of Company Equipment

Company equipment containing storage media must be verified to ensure that any CI and licensed software has been removed or securely overwritten prior to disposal or re-use.

5.7.3.1. Media Destruction

Data owners and asset custodians must sanitize media when it is no longer needed for business or legal reasons. Asset custodians must destroy media that cannot be sanitized, as follows:

- Shred, incinerate, or pulp hardcopy materials so that CI cannot be reconstructed; or
- Render data on electronic media unrecoverable so that data cannot be reconstructed.

Secure storage containers must be used for CI that is waiting to be destroyed.

5.7.4. Unattended User Company Equipment

Users must ensure that unattended company equipment has appropriate protection(s).

5.7.4.1. Device Storage in Automobiles

The Company shall require protection of mobile information systems away from Company premises. When traveling with Company-issued laptops and mobile devices, users will be required to:

- Lock the device(s) in the trunk of a user's automobile; or
- Maintain physical control and not leave the device(s) in the automobile.

5.8. Operations Security

The purpose of this section is to ensure the confidentiality, integrity, and availability of the Company's data through implementing appropriate technologies to protect information systems and data.

5.8.1. Change Management

Changes to the Company, business processes, information processing facilities, and systems that affect Information Security must be controlled.

5.8.1.1. Configuration Change Control

The Company shall:

- Determine the types of changes to information systems that are configuration controlled;
- Approve configuration-controlled changes to systems with explicit consideration for security impact analyses;
- Document approved configuration-controlled changes to systems;
- Retain and review records of configuration-controlled changes to systems;
- Audit activities associated with configuration-controlled changes to systems; and

Asset custodians and data owners will be required to test, validate, and document changes to information systems before implementing the changes on the production network.

5.8.1.2. Prohibition of Changes

The Company shall employ mechanisms to:

- Document proposed changes to information systems;
- Notify organized-defined approval authorities;
- Prohibit changes to information systems until designated approvals are received; and
- Document completed changes to information systems.

5.8.1.3. Security Impact Analysis for Changes

The Company shall analyze changes to information systems to determine potential security impacts prior to change implementation.

5.8.2. Controls Against Malware

Detection, prevention and recovery controls to protect against malware must be implemented, combined with appropriate user awareness.

5.8.2.1. Anti-malware Installation

Asset custodians shall deploy Company-approved anti-malware software on all systems capable of running anti-malware software, including, but not limited to:

- Workstations;
- Servers;
- Tablets;
- Mobile phones.

5.8.3. Information Backup

Backup copies of information, software, and system images must be taken and tested regularly.

5.8.3.1. Information System Recovery & Reconstitution

The Company's IT department shall provide for the recovery and reconstitution of information system to a known state after a disruption, compromise, or failure.

5.8.3.2. Information System Imaging

The Company's IT department shall provide the capability to re-image information systems from configuration-controlled and integrity-protected disk images representing a secure, operational state for the system.

5.8.4. Event Logging

Event logs recording user activities, exceptions, faults, and information security events must be produced, kept, and regularly reviewed.

5.8.4.1. Audit Trail Content

Asset custodians must configure systems to record at least the following audit trail entries for all system components, for each event where possible:

- User identification;
- Type of event;
- Date and time;
- Success or failure indication;
- Origination of event; and
- Identity or name of affected data, system component, or resource.

5.8.4.2. Log Review

Data owners and asset custodians must develop and implement a process to review logs and security events for all system components, and to identify anomalies or suspicious activity that includes:

a) Reviewing the following, on a periodic basis when logs are available:
   - All critical security events;
   - Logs of all critical system components that store, process, or transmit CI, or that could impact the security of CI;
   - Logs of all critical system components; and
   - Logs of all servers and system components that perform security functions. This includes, but is not limited to:
     1) Firewalls
     2) Intrusion Detection Systems (IDS)
     3) Intrusion Prevention Systems (IPS)
     4) Authentication servers (e.g., Active Directory domain controllers); and
   - Following-up on exceptions and anomalies identified during the review process.

5.8.5. Protection of Log Information

Logging facilities and log information must be protected against tampering and unauthorized access.

5.8.5.1. Securing Audit Trails

Asset custodians must secure audit trails so the logs cannot be altered. Securing audit trails includes the following:

- Limiting viewing of audit trails to those with a job-related need; and
- Protecting audit trail files from unauthorized modifications.

5.8.5.2. Retention of Audit Trail History

Data owners and asset custodians must retain audit trail history for at least three (3) years, with a minimum of three (3) months immediately available for analysis.

5.8.6. Clock Synchronization

The clocks of all relevant information processing systems within a Company or security domain must be synchronized to a single reference time source.

5.8.6.1. Network Time Protocol (NTP)

a) Asset custodians must configure the Company's NTP servers so that they are receiving time from industry-accepted time sources; and

b) Asset owners must ensure NTP on their systems is configured properly.

5.8.7. Installation of Software or Hardware on Operational Systems

Procedures must be implemented to control the installation of software or hardware on operational systems.

Asset custodians must configure information systems to prevent the installation of software and hardware components by non-administrators through limiting the actions that users can perform.

5.8.7.1. Standardized Images

Unless a technical or business reason exists, standardized images will be used to represent hardened versions of the underlying operating system and the applications installed on the system. These images must be validated and refreshed on a regular basis to update their security configuration.

Any exception requests that deviate from the standard image for laptops and desktops, must be submitted to loanDepot's Chief Information Security Officer (CISO) at *ISO@loanDepot.com* for approval.

5.8.8. Management of Technical Vulnerabilities

Information about technical vulnerabilities of information systems being used must be obtained in a timely fashion, the Company's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

5.8.8.1. Software Patching

Asset custodians must ensure that:

a) All system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed;

b) Critical/High security patches are installed within thirty (30) calendar days of the vendor's release data; and

c) Non-critical security patches are installed within ninety (90) calendar days of the vendor's release data.

5.8.8.2. Vulnerability Scanning

The Information Security team shall establish a Vulnerability Management program that will regularly scan the IT environment for known vulnerabilities. Findings shall be reported to respective asset custodians for remediation or mitigation as appropriate.

5.8.9. Restrictions on Software and Hardware Installation

Rules governing the installation of software and hardware by users must be established and implemented.

Only system administrators and users with explicit privileged status will be permitted to install software or hardware.

Where technically feasible, alerting shall be configured to notify appropriate asset custodians or Information Security personnel when the unauthorized installation of software or hardware is detected.

5.9. Communications Security

The purpose of this section is to ensure sufficient mechanisms are in place to protect the confidentiality and integrity of the Company's communications.

5.9.1. Network Controls

Networks must be managed and controlled to protect information in systems and applications.

5.9.1.1. Firewall & Router Configurations

Information Security must establish firewall and router configuration standards that include the following:

a) Information Security must establish and maintain a formal process for approving and testing all network connections and changes to both firewall and router configurations; and

b) Network diagrams must be updated as changes are approved and implemented by appropriate personnel.

5.9.1.2. Safeguarding Data over Open Networks

The Company shall use strong cryptography and security protocols to safeguard Personally Identifiable Information (PII) during transmission over open, public networks.

To safeguard PII during transmission, asset custodians must ensure the following:

a) Strong cryptography and security protocols must safeguard CI during transmission over open, public networks; and

b) Wireless networks transmitting PII or connected to sensitive networks, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission.

5.9.2. Security of Network Services

Security mechanisms, service levels and management requirements of all network services must be identified and included in network services agreements, whether these services are provided in-house or outsourced.

5.9.3. Agreements on Information Transfer

Agreements must address the secure transfer of business information between the Company and external parties.

The Company shall:

a) Ensure that individuals requiring access to CI and information systems sign appropriate access agreements prior to being granted access; and

b) Review/update the access agreements.

The Company shall ensure that access to information with special protection measures is granted only to individuals who:

a) Have a valid access authorization; and

b) Satisfy associated user security criteria.

5.9.4. Electronic Messaging

Information involved in electronic messaging must be appropriately protected.

5.9.4.1. Transmission Confidentiality

The Company shall protect the confidentiality of transmitted PII. Asset custodians and data owners will be required to employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.

5.9.4.2. Ad-Hoc Transfers

The Company shall employ a technology-based method for securely exchanging large files with external parties. Unscheduled, infrequent, and one-time file transfers that contain CI are required to be performed through encrypted transport protocols.

5.9.5. Confidentiality or Non-Disclosure Agreements

Requirements for confidentiality or non-disclosure agreements reflecting the Company's needs for the protection of information must be identified, regularly reviewed and documented.

5.9.5.1. Business Partner Contracts

If the Company shall permit a business partner to create, receive, maintain, or transmit CI on the Company's behalf, approval from the Information Security department must be obtained before the transmission of data takes place. The Company shall obtain satisfactory assurances from the business associate that appropriate safeguards are in place and enforced.

The Company shall maintain written and executed agreements with business partners to ensure:

a) Appropriate management, operational, and technical control safeguards are in place to ensure the confidentiality, integrity, and availability of the CI the business associate creates, receives, maintains, or transmits; and

b) Service providers acknowledge in writing that they are responsible for the security of CI that the service provider possesses or otherwise stores, processes, or transmits on behalf of the Company, or to the extent that they could impact the security of the Company data environment.

5.9.5.2. Third Party Personnel Security

The Company shall:

a) Prohibit the use of non-Company laptops, and

b) Monitor provider compliance.

The Company must ensure third party user access is granted only to individuals who:

a) Have a valid access authorization;

b) Have read, understand, and signed a Non-Disclosure Agreement (NDA); and

c) Have read, understand, and signed an acknowledgement that he or she understands and will abide by the Company's policies, procedures, standards, and guidelines.

5.10. System Acquisition, Development and Maintenance

The purpose of this section is to ensure that information systems employ a System Development Life Cycle (SDLC), where the security of systems and services are assessed throughout their operational life to reduce risks to the Company.

5.10.1. Information Security Requirements Analysis and Specification

The Information Security-related requirements must be included in the requirements for new information systems or enhancements to existing information systems. Any new or planned application must have an application security assessment performed prior to going live. Remediation must be completed for critical and high-risk issues as a result of an application security assessment.

5.10.1.1. Secure Configurations

Information Security must develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production hardening systems includes, but is not limited to:

a) Verifying that system configuration standards are:
   - Updated as new vulnerability issues are identified;
   - Applied when new systems are configured; and
   - Consistent with industry-accepted hardening standards;

b) Enforcing least functionality, which includes but is not limited to:
   - Allowing only necessary and secure services, protocols, and daemons; and
   - Removing all unnecessary functionality.

5.10.2. Security in Development and Support Processes

The Company shall ensure that Information Security is designed and implemented within the development lifecycle of information systems.

Data owners and asset custodians must ensure that internal and external developers:

a) Incorporate Information Security throughout the software development life cycle;

b) Remove custom application accounts, user IDs, and passwords before applications become active or are released to customers; and

c) Review custom code or perform application level vulnerability scanning prior to release to production or customers in order to identify any potential coding vulnerability.

5.10.3. System Change Control Processes

Changes to systems within the development lifecycle must be controlled by the use of formal change control processes.

The Company's asset custodians must follow change control programs for all changes to system components and ensure that back-out procedures are provided as needed.

5.10.4. System Acceptance Testing

Acceptance testing programs and related criteria must be established for new information systems, upgrades, and changes.

5.10.5. Protection of Test Data

Test data must be selected carefully, protected, and controlled.

The Company shall scramble, redact, approve, document, and control the use of live data in development and test environments for the information system, system component, or information system service.

The Company shall document processes to ensure the integrity of test through existing security controls. Developers, in conjunction with the Company's Information Security personnel, must implement appropriate mechanisms to protect the integrity of test data.

5.11. Vendor Management

The purpose of this section is to ensure that risk associated with outsourced service provider relationships are minimized or eliminated. As service providers' people, technology, and practices evolve over time, the Company must ensure the appropriate levels of due care and due diligence are applied to validate Information Security controls are effective.

5.11.1. Information Security Policy for Supplier Relationships

Information Security requirements for mitigating the risks associated with supplier's access to the Company's assets must be agreed to with the supplier and documented.

5.11.1.1. **Service Provider Management**

The Company shall maintain and implement programs to manage service providers with whom CI is shared, or that could affect the security of CI. Vendor Management must maintain and implement procedures to manage service providers that include, but are not limited to:

a) Maintaining a list of service providers;

b) Maintaining a written agreement that includes: (i) an acknowledgement that the service providers are responsible for the security of CI the service providers possess or otherwise store, process, or transmit on behalf of the Company, or to the extent that they could impact the security of the Company and (ii) appropriate contractual protections and remedies with respect to maintaining the privacy and security of data.

c) Ensures there is an established process for engaging service providers, including proper due diligence prior to engagement;

d) Maintaining a program to monitor service providers' compliance status at least annually; and

e) Maintaining information about which requirements are managed by each service provider, and which are managed by the Company.

5.11.1.2. **Acquisition Process**

The Company shall include the following requirements and/or specifications, explicitly or by reference, in information system acquisitions based on an assessment of risk over the security functional requirements/specifications.

Asset custodians and data owners must take security requirements into account when purchasing information systems or outsourcing solutions and include appropriate contractual protections and remedies with respect to maintaining the privacy and security of data.

5.11.2. Addressing Security Within Supplier Agreements

All relevant Information Security requirements must be established and agreed to with each supplier that may access, process, store, communicate, or provide IT infrastructure components for CI.

Topic	Requirement
Service Provider Accountability	Service providers must acknowledge in writing to the Company that they are responsible for the security of CI that they possess or otherwise store, process, or transmit on behalf of the Company, or to the extent that the service provider could impact the security of the Company.
Liability from Harm	Responsible parties within the Company shall employ safeguards to limit harm from Information Security threats to the supply chain.

5.11.2.1. Development Process, Standards, & Tools

The Company must require the implementation of industry-recognized best practices throughout the Software Development Life Cycle (SDLC) in line with LD's policy and practices.

5.12. Incident Response

The purpose of this section is to establish and maintain a capability to guide the Company's response when cyber-security incidents occur.

5.12.1. Responsibilities and Procedures

Management responsibilities and procedures must be established to ensure a quick, effective, and orderly response to Information Security incidents.

5.12.1.1. Incident Response

The Company shall:

a) Implement an Incident Response (IR) capability that is prepared to respond immediately to potential cyber security incidents.

b) Create an IR plan that is capable of being be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise;
- Specific incident response procedures;
- Analysis of legal requirements for reporting compromises; and
- Coverage and responses of all critical system components.

c) Test the IR plan at least annually.

d) Designate IR personnel to be available on a 24/7 basis to respond to alerts.

e) Provide appropriate training to staff with security breach response responsibilities and to all staff on how to report suspicious events.

f) Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

5.12.2. Response to Information Security Incidents

Information Security incidents must be responded to in accordance with the documented procedures.

The Company shall maintain an incident response plan that provides a high-level approach for how the plan works and engages stakeholders to manage risk throughout the process.

5.13. Information Security Compliance

The purpose of this section is to supplement the management, operational, and technical security controls to ensure safeguards are in place to specifically protect CI collected or maintained by the Company against loss, unauthorized access, or disclosure.

5.13.1. Identification of Applicable Legislation and Contractual Requirements

All relevant legislative statutory, regulatory, contractual requirements, and the Company's approach to meet these requirements must be explicitly identified, documented, and kept up to date for each information system and the Company.

5.13.1.1. Minimizing Company Information Storage

The Company must implement a process to minimize the storage of CI. The Company's data owners must determine the business requirements for data retention and securely dispose of CI once the data is no longer necessary. This includes, but is not limited to:

a) Implementing a data retention and disposal procedure that covers CI handling;

b) Limiting data retention time to that which is required for legal, regulatory, and business requirements;

c) Conducting an annual process (automatic or manual) to identify and securely delete stored CI that exceeds defined retention requirements;

d) Performing secure deletion of electronic-based CI; and

e) Shredding physical-based CI.

5.13.1.2. Data Masking

The Company shall apply data masking to CI that is displayed or printed, where possible (see *Data Handling Procedure* for more information). This includes, but is not limited to the following:

a) Personally Identifiable Information (PII)

b) Financial account numbers

c) Social Security Numbers (SSN)

d) Driver's License Numbers

e) Making Company Information Unreadable In Storage

Asset custodians must implement technical measures to ensure CI is not accessible by unauthorized users or processes.

5.13.2. Privacy and Protection of Company Information

Privacy and protection of CI must be ensured as required in relevant legislation and regulation where applicable.

5.13.2.1. Minimization of Company Information

The Company shall:

a) Identify the minimum CI elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the purpose of collection.

AND

b) Limit the collection and retention of CI to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.

Where feasible and within the limits of technology, data owners are responsible for locating and removing/redacting unnecessary CI through the use of anonymization and de-identification techniques.

5.13.2.2. Data Retention & Disposal

The Company shall use the Records Retention policy to:

a) Retain CI for a defined time period to fulfill the purpose(s) identified in the notice or as required by law.

b) Dispose of, destroy, erase, and/or anonymize the CI, regardless of the method of storage.

c) Use defined techniques or methods to ensure secure deletion or destruction of CI (including originals, copies, and archived records).

5.13.2.3. Data Collection

Data owners must implement limitations on the collection, use, and disclosure of personal information.

5.13.3. Regulation of Cryptographic Controls

Cryptographic controls must be used in compliance with all relevant agreements, legislation, and regulations.

5.13.4. Independent Review of Information Security

The Company's approach to managing Information Security and its implementation (e.g., control objectives, controls, policies, processes, and procedures for Information Security) must be reviewed independently at planned intervals or when significant changes occur.

The Company shall employ assessors or assessment teams with independence to conduct security control assessments. Whenever feasible, the Company will utilize independent assessors for security assessment functions.

5.13.5. Compliance with Security Policies and Standards

Managers must regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

5.13.5.1. Security Assessments

The Company shall:

a) Assess the security controls in information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

b) Produce a security assessment report that documents the results of the assessment.

c) Provide the results of the security control assessment, in writing, to the CISO.

A formal Information Security risk analysis must be performed on all significant development and/or acquisitions, prior to information systems being placed into production:

a) New information systems and applications must be appropriately tested for functionality prior to being placed in production.

AND

b) Asset custodians and data owners will be required to perform a gap analysis, at least once per year, to determine any deviations between their systems' current state of compliance and that which is required.

5.14. Acceptable Use

The Company does not impose restrictions that are contrary to its established culture. The Company shall commit to protecting employees and CI from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with Company information resources. It is the responsibility of every user to know these requirements and to conduct activities accordingly.

This section shall outline the acceptable use of Company information resources. These requirements are in place to protect the employee and the Company. Inappropriate use exposes the Company to risks including virus attacks, compromise of information systems, and legal issues.

5.14.1. Clean Desk

a. Work areas must be cleared of all sensitive data when not occupied.

b. All CI must be removed from desks and locked in a drawer, filing cabinet, or other secured/restricted area at the end of each workday.

5.14.2. General Use and Ownership

CI stored on Company information resources is the sole property of LD. The Company shall ensure through legal or technical means that CI is protected.

Company personnel shall promptly report the theft, loss, or unauthorized disclosure of CI. CI may be accessed, used, or shared only to the extent it is authorized and necessary to fulfill assigned job duties.

5.14.2.1. Reasonable Non-business Use of Online Services

Reasonable or occasional non-business use of Online Services is permitted, provided it does not conflict with business objectives, policies, and guidelines of the Company, and provided it is not an abuse of the Company's time or resources. Users must not use Online Services to run a personal business, even if such a personal business is declared in a conflicts of interest statement (see *Section 5.14.23* for more information).

5.14.2.2. Security and Company Information

a) System level and user level passwords must comply with *Section 5.5.6 Password Management*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

b) All computing devices must be secured with a password-protected screensaver with the automatic activation feature. Users must lock the screen or log off when the device is unattended.

c) Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is in the course of business duties.

d) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

5.14.2.3. Remote Printing

CI may only be printed when business justifies it. If printed, it must be adequately secured, and shredded when no longer needed.

5.14.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., Information Security may disable the network access of a host if that host is disrupting production services).

Under no circumstances are personnel authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Company information resources. The Company prohibits access to internet sites that are considered illegal or inappropriate. An Information Security exception request can be submitted if there is a legitimate business purpose for access to a blocked site (*see 5.15 Exceptions*).

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

5.14.3.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a) Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by the Company.

b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the end user does not have an active license is strictly prohibited.

c) Accessing data, a server, or an account for any purpose other than conducting Company business, even if you have authorized access, is prohibited.

d) Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

e) Introduction of malware into the network or server.

f) Revealing account password to others or allowing use of user account by others. This includes family and other household members when work is being done at home.

g) Using a Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

h) Making fraudulent offers of products, items, or services originating from any Company account.

i) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

j) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

k) Port scanning or security scanning is expressly prohibited.

l) Executing any form of network monitoring which will intercept data, unless this activity is a part of the employee's normal job/duty.

m) Circumventing user authentication or security of any host, network, or account.

n) Sharing CI with non-approved parties outside the Company.

o) Sharing CI outside approved business processes.

p) Storage of Company Information is prohibited in non-Company managed locations such as personal drives, personal cloud storage, and devices.

q) Accessing Company resources using anonymizing services such as third-party VPNs, hiding or otherwise masking their electronic activity on company devices and networks via third-party services such as personal VPNs and anonymizing services.

r) Activities involving gambling, gaming and/or any other activity with an entry fee and a prize, including, but not limited to casino games, sports betting, horse or greyhound racing, fantasy sports, lottery tickets, other ventures that facilitate gambling, games of skill (whether or not legally defined as gambling) and sweepstakes.

5.14.3.2. Email and Communication Activities

When using Company information resources to access and use the Internet, users must realize they represent the Company. Whenever employees state an affiliation to the Company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be addressed to *ISO@loanDepot.com* (see *Section 5.14.2.3* for more information on social media use).

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material, to individuals who did not specifically request such material (email spam).

a) Any form of harassment via email or telephone, whether through language, frequency, or size of messages.

b) Unauthorized use or forging of email header information.

c) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

d) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

e) Use of unsolicited email originating from within the Company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Company or connected via the Company's network.

f) The sending of commercial email messages, including but not limited to, bulk advertisements, promotions, product updates, etc. must be done through the appropriate marketing channels due to extensive compliance requirements.

g) Posting the same or similar non-business-related messages to large numbers of Usenet groups (newsgroup spam).

h) Auto-forwarding email rules to external third parties, including personal email accounts, is prohibited.

5.14.3.3. Blogging and Social Media

a) Blogging by employees, whether using the Company's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the Company's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Company's policy, is not detrimental to the Company's best interests, and does not interfere with an employee's regular work duties. Blogging from the Company's systems is also subject to monitoring.

b) The Company's *Data Classification Policy* and *Data Handling Procedure* also applies to blogging. As such, Company personnel are prohibited from revealing any Confidential, or proprietary information, trade secrets, or any other material covered by the *Data Classification Policy* and *Data Handling Procedure* when engaged in blogging.

c) Regarding your personal use of social media and blogging, while your free time is generally not subject to any restriction by the Company, the Company urges all employees not to post information regarding the Company, their jobs, or other employees which could lead to morale issues in the workplace or detrimentally affect the Company's business. This can be accomplished by always thinking before you post, being civil to others and their opinions, and not posting personal information about others unless you have received their permission. You are personally responsible for the content you publish on blogs, wikis, or any other Social Media Sites. Be mindful that what you publish will be public for a long time. Also recognize that if the Company receives a complaint from an employee about information you have posted about that employee, the Company may need to investigate that complaint to ensure that there has been no violation of the harassment policy or other Company policy. In the event there is such a complaint, you will be expected to cooperate in any investigation of that complaint, including providing access to the posts at issue.

d) Personnel are prohibited from making any unlawful, discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited.

e) Personnel may also not attribute personal statements, opinions, or beliefs to the Company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of LD. Employees assume any and all risk associated with blogging.

f) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the Company's trademarks, logos, and any other Company intellectual property may also not be used in connection with any blogging activity.

5.14.4. Monitoring of Users

The Company shall reserve the right, subject to local laws and regulations, to review, audit, monitor, intercept, access, and disclose all uses of its Company Information Resources, and in particular, email,

voicemail, Instant Messaging Services (e.g. WebEx), Internet use, and all files or information stored on Company Equipment, without prior notification to the user(s) concerned, provided that such monitoring will be done:

a) To protect the security of the Company, its customers, suppliers, and employees.

b) To protect and maintain proper operation and use of the assets of the Company.

c) To investigate unauthorized access to or use of Information Resources.

d) For an urgent, legitimate business need (e.g. employee unavailable and timing critical, or to access CI after an employee has left the Company).

e) To investigate a reasonable suspicion of violation of law or policy of the Company, by a user or ex-user.

f) To respond to a subpoena or government investigation or otherwise comply with applicable laws or regulations.

g) To monitor quality and to assure compliance with regulatory requirements and customer obligations.

In this regard, users shall have no expectation of privacy in connection with their use of the Company's information technology systems, networks, and devices. A failure to monitor in a particular situation shall not be deemed a waiver of the right to monitor in other similar situations.

The Company shall reserve the right to carry out other forms of monitoring of use or access to its Company information resources.

If the Company discovers any user misconduct (including any violation of this or any other policy or guideline of the Company) or criminal activity involving Company information resources, the files or information related to such conduct shall be used to document the conduct and may be disclosed to appropriate authorities.

The Company shall not use any monitoring devices or other means to attempt to discover the identity of anyone using an ethics hotline or any other complaint reporting tool advertised as allowing anonymous reporting and will not do so unless required by law or court order.

The Company also shall not intend to monitor, review or disclose communications between employees and their personal attorneys; however, the Company must disclaim any and all liability for any inadvertent access to or disclosure of such communications.

5.14.5. Reporting of Violations and Incidents

Inappropriate Use, Theft, Misappropriation or Other Incidents: Users shall immediately notify *ISO@loanDepot.com* of any unusual behavior pertaining to Company Information Resources, subject to local law and any legal restrictions on such reporting.

5.14.6. Suppliers, Contractors and Other Third Parties

This policy applies to the use of CI, Company Equipment, and Online Services by suppliers, contractors, and other third parties, subject to any particular contractual arrangement in place with such third parties and any other external legal obligation that may exist under the local law of the third party.

5.14.7. Questions About Acceptable Use

For questions about this section, please email *ISO@loanDepot.com*.

5.15. Exceptions

Request for exceptions to this policy or any other Information Security policy or procedure shall be submitted through mello assist using the Information Security Exception request form and approved by the Chief Information Security Officer or their designee. Prior to approval of any exception, the policy must continue to be followed. Exceptions are valid for a specified time period, with a one-year (1) period being the maximum time period.

5.15.1. Exception Request and Approval Process

A User seeking an exception, must assess the risks that non-compliance creates for the Company. If their manager believes the risk is reasonable, the user shall prepare a written request describing the business justification for an exception. This request must include an approval from the requestors' SVP or above.

Exceptions can be granted when compliance with a policy adversely affects business objectives or when the cost to comply offsets the risk of non-compliance and the exception will not have a regulatory impact.

The risk analysis shall include:

- Identification of the threats and vulnerabilities, how likely each is to occur, and the potential costs of an occurrence.
- The cost to comply with the policy requirements.

The request for an exception is originated in ServiceNow and must include supporting documentation and risk analysis. The Cyber Security manager or designee shall conduct a security review and make a recommendation. In some instances, key stakeholders such as managers, asset custodians, and legal representatives will be involved.

- The executive approver will use the cyber security review and recommendation to approve or decline the request, and the requestor will be notified.
- All exception requests will be retained in ServiceNow, and approved exceptions will be tracked autonomously in the Information Security Exception Tracker spread sheet.

The following automated notifications are sent as the exception period lapses.

- 30 days prior to expiration – automated ServiceNow renewal notification is sent to the requestor.
- 2 weeks prior to expiration – automated ServiceNow renewal notification is sent to the requestor and their manager.
- Day of expiration – automated ServiceNow deactivation notification to the requestor, their manager, and the Cyber Security group.

Renewal requests create a new record in ServiceNow that is tied to the original request. The Cyber Security reviewer shall determine whether the conditions that justified the original exception approval are still in effect and gather new information as needed following the same steps as with the original request.

5.16. Risk Management Framework

The Company maintains an information security risk management program to evaluate threats and vulnerabilities in order to assure the creation of appropriate remediation plans.

5.16.1. Risk Management Overview

There is sometimes conflict between information security and other general system/software engineering principles. Information security can sometimes be construed as interfering with ``ease of use'' where installing security counter measures take more effort than a ``trivial'' installation that works but is insecure. Often, this apparent conflict can be resolved by re-thinking the problem and it is generally possible to make a secure system also easy to use. Based on the value owners place on their assets, it is a necessity to impose countermeasures to mitigate any risks posed by specific threats.

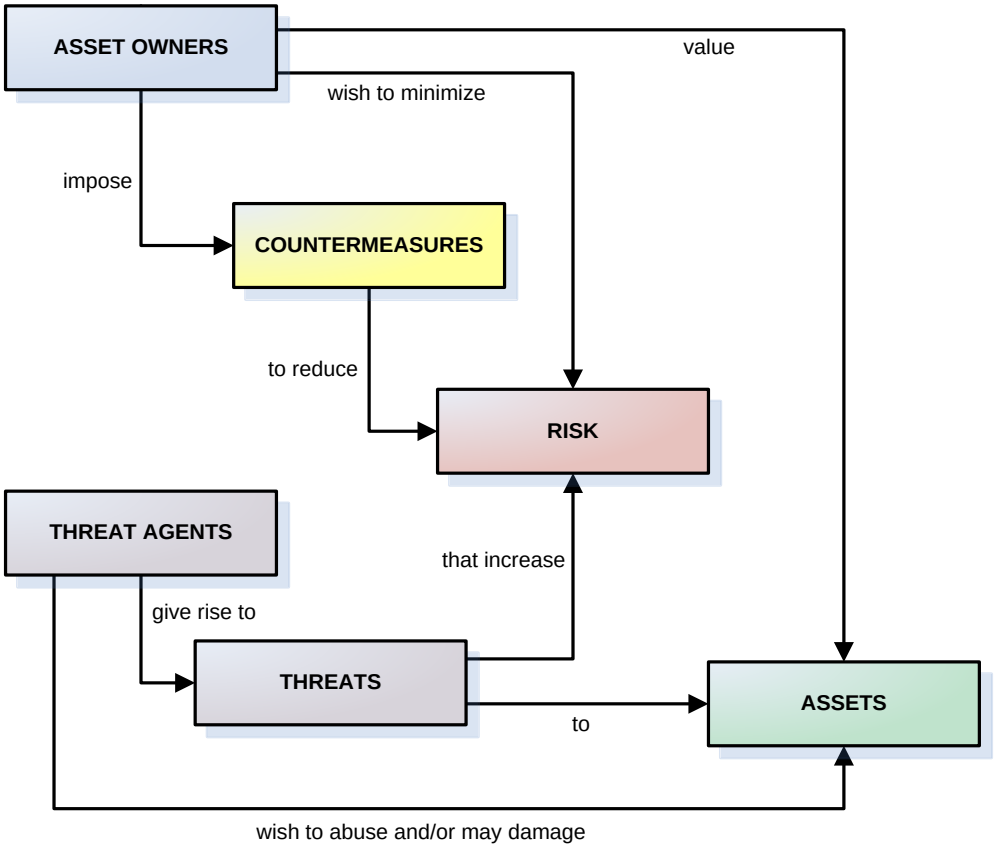

Figure 1: Risk Overview

5.16.2. Risk Management Framework (RMF)

Risk management requires finding security equilibrium between vulnerabilities and acceptable security controls. This equilibrium can be thought of as acceptable risk – it changes as vulnerabilities and controls change. From a systems perspective, the components used to determine acceptable risk cover the entire Defense-in-Depth (DiD) breadth. If one component is weakened, another component must be strengthened to maintain the same level of security assurance. Risk management activities can be applied to both new and legacy information systems.

The Risk Management Framework (RMF) is based off of NIST SP 800-371:

- **Categorize**. The information system and the information being processed, stored, and transmitted by the system, based on the potential impact to the organization should events occur to put the system

[1] http://csrc.nist.gov/publications/PubsSPs.html

and its information at risk. The organization assigns a security impact value (low, medium, high) for the security objectives of confidentiality, integrity, or availability for the information and information systems that are needed by the organization to accomplish its mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.

- **Select**. An appropriate set of security controls are selected for the information system after categorizing and determining the minimum-security requirements. Organizations meet the minimum-security requirements by selecting an appropriately tailored set of baseline security controls, based on an assessment of risk and local conditions, including the organization's specific security requirements, threat information, cost-benefit analyses, or special circumstances.

- **Implement**. Security controls must be properly installed and configured in the information system. Checklists of security settings are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is a series of instructions for configuring an IT product to an operational environment.

- **Assess**. Security Testing & Evaluation (ST&E) is used to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Authorize**. Based upon a determination of the risk to operations, organizational assets, or to individuals resulting from the operation of the information system, and the determination that this risk is acceptable.

- **Monitor**. Assessing selected security controls in the information system on a continuous basis, including documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to appropriate organization officials on a regular basis.

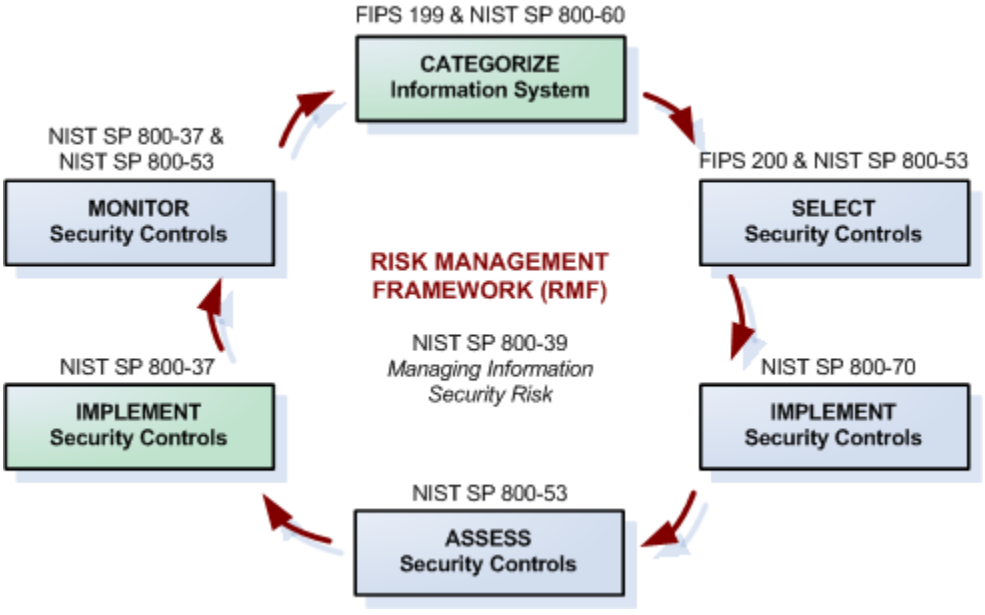

Figure 2: Risk Management Framework (RMF)

5.16.3. Assessing Risk

LD management must ensure that Risk Assessments (RAs) are conducted to identify the critical assets that require protection, and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. RAs should take into account the potential adverse impact on LD's reputation, operations, and assets. RAs should be conducted by personnel associated with the activities subject to assessment.

RAs can be conducted on any system or project internal or external to LD, including applications, servers, networks, and any process or procedure by which these systems are administered and/or maintained. LD encourages authorized, periodic RAs for the purpose of determining areas of vulnerability and to initiate appropriate remediation.

The execution, development, and implementation of remediation programs are the responsibility of LD's management. Users are expected to cooperate fully with any RA being conducted on systems for which they are held accountable.

A method of assessing risk is to identify the likelihood of an event actually taking place and the consequences that would result from the incident occurring.

While assessing the likelihood and consequence of an event is sometime more subjective, rather than based on quantifiable data, the following figures should be used to assess risk:

Rating Risk	EXTREME - detailed response plan & employee training required
	HIGH – requires management attention and response plan
	MODERATE – significant impact to overall operations
	LOW – managed by routine procedures
Likelihood	CERTAINTY - expected in most circumstances (matter of time)
	LIKELY – will probably occur in most circumstances
	POSSIBLE – could occur at some time
	UNLIKELY – not expected to occur
	RARE – exceptional circumstances only
Consequences	SEVERE – would stop achievement of functional goals & objectives
	MAJOR – would threaten functional goals & objectives
	MODERATE – significant impact to overall operations
	MINOR – would threaten an element of operations
	NEGLIGIBLE – minor impact on productivity

Figure 3: Standardizing Terminology

Occurrence Probability		Occurrence Consequence				
		Negligible	**Minor**	**Moderate**	**Major**	**Severe**
	Certainty	L	M	H	E	E
	Likely	L	M	H	E	E
	Possible	L	M	M	H	E
	Unlikely	L	M	M	M	H
	Rare	L	L	M	M	H

Figure 4: Risk Matrix

6. Policy Violations

Any personnel found to have violated any policy or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, federal, and/or international law will be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

7. Controls

Information Security controls are identified within each section of the Policy Detail.

8. Accountability

All employees must adhere to this policy and must notify management concerning any practices that they believe to be inconsistent with this policy.

8.1. Policy Approval

The Chief Information Security Officer (CISO) is responsible for approving the creation, update, and retirement of this policy.

8.2. Senior Vice Presidents

The SVPs are accountable for overseeing departmental compliance with this policy. They also shall ensure Information Security is integrated into departmental processes and may delegate accountability to their Directors.

8.3. Vice Presidents

The VPs are responsible for driving the Information Security program to ensure their staff is aware of all policy and procedural requirements and maintain compliance of the Information Security Policy.

9. Maintenance of Records

All records must be kept in accordance with the Company's Records Retention Schedule.

10. Revision History

Initiated By	Version #	Effective Date	Change Description
Information Security	1	12/29/17	• New document
Information Security	2	6/30/2018	• Updated Personally Owned Device Section 5.5.2.2.2, table and formatting issues, and added hyperlinks to additional policies and procedures that have been published.
`	3	11/9/2018	• Updated Section 5.5.6 Password Management User Accounts: Minimum of eight (8) characters. (changed from 6 to 8 characters) • Updated Section 5.8.7 Installation of Software or Hardware on Operational Systems (added Hardware) • Updated Section 5.5.2.2.3 Restrictions on Software and Hardware Installation (added Hardware) • Updated Section 5.8.9 Added Teleworkers shall only access company resources from company-issued or approved personal devices. Accessing company resource through anonymizing services such as personal VPNs is strictly prohibited. • Added Section 5.14.2.1.o " The following activities are strictly prohibited, with no exceptions" Accessing company resources using anonymizing services such as third-party VPNs.
Information Security	5	7/17/2019	• Added Section 5.14.1 Clean Desk • Updated Section 5.14.3.2, added (g) Auto-forwarding email rules prohibited, added language around the sending of bulk commercial email, and added language around the sending of bulk commercial email • Updated Section 5.8.7.1 added CISO approval for non-Standard PC and laptop images • Updated Section 5.14.2.3 added language regarding remote printing of Company documents • Updated Section 5.14.3.1 added language around the sharing of personnel information, storing Company data on personal drives; the use of anonymizing services on Company devices/networks; engaging in activities on Company devices/networks involving gambling. • Updated Addendum 11 with "Teams Involved" in Incident Responses and added Priority Overview for Information Security and Network
Information Security	5.1	9/13/2019	• Updated 5.14.3 to add language about the Company blocking illegal or inappropriate sites. • 5.5.6 removed minimum password life
Information Security	5.2	12/4/2019	• Updated 5.5.6 - minimum length of password requirements from 9 to 10
Information Security	6	07/08/2020	• Updated 5.5.2.2.2 – updated to require employee owned devices be connected to guest Wi-Fi; • Updated 8.1 - Policy Approver • Updated 5.15 - Exceptions

11. Addendum

11.1. Incident – Prioritization Overview

Priority	Impact	Response Time	Teams Involved (at a minimum)	Resolution Time	Requirement
P - 1 N - 1 S - 1	Critical – Major Incident	Instant - *Must be Called In to SD*	Major Incident Core Team, Service Desk, Network Team, InfoSec	2 Hours	• Major Enterprise Applications degraded or unusable OR • More than 200 people affected by an issue OR • Revenue is being significantly impacted
P - 2 N - 2 S - 2	High – Major Incident	Instant - *Must be Called In to SD*	Major Incident Core Team, Service Desk, Network Team, InfoSec	6 Hours	• Local Application outage or partial degradation of Enterprise Application OR • At least 30% of a single branch is affected OR • Revenue is being moderately impacted
P - 3 N - 3 S - 3	High – Individual	2 Hours	Service Desk	2 Business Days	• Impact to an individual or application impacting a required deadline • An issue impacting less than 30% of an entire site • Lost or stolen equipment • Issues stopping a loan in progress
P - 4 N - 4 S - 4	Medium	1 Business Day	Service Desk	3 Business Days	• Individual impact with medium urgency • Non loan-stop issues • Reduces productivity without impacting deadlines
P - 5 N - 5 S - 5	Low	1 Business Day	Service Desk	7 Business Days	• Minor nuisance or inconvenience • Questions or training requirement

P: Infrastructure Incident

N: Network Incident

S: Security Incident

Priority levels 1 and 2 are Major Incidents. The Root Cause, Resolution, and Future Preventative Steps are presented and discussed biweekly, at the Major Incident Review meeting.

11.2. Glossary of Information Security Terms & Concepts

Term	Concept
Access Control	A process that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: • Pass the information to other subjects or objects; • Grant its privileges to other subjects; • Change security attributes on subjects, objects, information systems, or system components; • Choose the security attributes to be associated with newly-created or revised objects; or • Change the rules governing access control.
Asset	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g. user password or token).
Authorization (to operate)	Official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorization Boundary	All components of an information system to be authorized for operation and excludes separately authorized systems, to which the information system is connected.
Availability	Ensuring timely and reliable access to and use of information. Loss of availability is the disruption of access to or use of information or an information system.
Company Equipment	This consists of the following components: • **Hardware** – desktops, servers, peripherals and any other device that connects to the Company network/infrastructure such as printers, copiers, video conferencing systems, CCTV, and wireless network equipment, that is purchased, provided, paid for or otherwise approved by the Company for business use by users, or otherwise used in connection with CI. • **Portable Devices** – Any type of electronic device that is meant to be carried rather than kept stationary, such as laptops, cell phones, tablet computers, and Removable data Storage Media, that is purchased, provided or approved by the Company for

	business use by a user, or any other such device that is used in connection with CI. • **Telecommunications Equipment** – Company telephone services (including voicemail), facsimile machines and related telecommunications hardware purchased, provided or approved by the Company for business use by users, or otherwise used in connection with CI.
Company Information (CI)	Information resources that are maintained in electronic, digital or hard-copy format. Company Information may be accessed, searched, or retrieved via electronic networks, data processing technologies, or other manual methods. This information includes, but is not limited to, the following types of Sensitive Information: • Non-Public Personal Information (NPI), Consumer personally identifiable information (PII), Customer PII, Employee PII, Intellectual Property (IP), Proprietary Information (PI), and Company business information, including the information of third-parties.
Company Information Resources	Resources that include CI, Company Equipment, Software, and Online Services as well as Personal Devices, as defined under Company Equipment.
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Control	Any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help the Company accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.
Control Objective	Targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, control objectives are directly linked to an industry-recognized best practice to align the Company with accepted due care requirements.
Cryptography	Principles, means and methods for the transformation of data in order to hide their content, prevent authorized use, or prevent undetected modification.
Data	An information resource that is maintained in electronic or digital format. • Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. • A subcategory of information in an electronic format that allows it to be retrieved or transmitted.
Deny All	By default, until authorized, all access to systems is denied.
Developer	Includes the following:

	• Developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; vendors. **AND** • Product resellers, development of systems, components, or services can occur internally within organizations (e.g., in-house development or through external entities.
Disruption	For purposes of this policy, “disruption” includes, but is not limited to; network niffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
Encryption	The conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.
Event	Any observable occurrence in an information system.
Firmware	Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs.
File Transfer Protocol (FTP)	A protocol used to transfer files over the internet.
Guidelines	Recommended practices that are based on industry-recognized best practices. Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.
Hardware	The physical components of an information system.
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation, or imminent threat of violation of security or acceptable use requirements.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information Security Steering Committee	Ensures enterprise-wide information security programs. Aligns to corporate business objectives with strategic security investments in order to reduce duplication in security spending, provides oversight of the information technology infrastructure, and reduces security risks to the Company.
Information Security	The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Focus is on the Confidentiality, Integrity, and Availability (CIA) of data.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Information System	An asset; a system or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices. **Note:** Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
Information System Service	A capability provided by an information system that facilitates information processing, storage, or transmission.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
Integrity	Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. • A loss of integrity is the unauthorized modification or destruction of information.
ISO 27001	Provides a standard for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the Company's information security management system.
Least Privilege	The theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function. • Access must be granted only for the minimum amount of time necessary.
Malware	Short for malicious software, and designed to infiltrate, damage, or obtain information from a computer system without the owner's consent.
Media	Physical devices or writing surfaces including, but not limited to; magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Non-Public Personal Information	Personally identifiable financial information (i) provided by a consumer to a financial institution, (ii) resulting from a transaction or service performed for the consumer, or (iii) otherwise obtained by the financial institution. Excluded from the definition are; (i) publicly available information and (ii) any consumer list that is derived without using personally identifiable financial information.
Object	Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving

	information. Access to an object (by a subject) implies access to the information it contains.
Online Services	The Internet, intranets of the Company, email, and other online data services or collaboration tools such as WebEx, the Company Folders and the Company Libraries, and instant messaging solutions that are provided, purchased or approved by the Company for business use by users, or otherwise used in connection with CI.
Physical Access Control System	An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
Personal Device	Any type of Hardware, Portable Device, Telecommunications Equipment, Removable data Storage Media or Online Service that is purchased or supplied by a user – without reimbursement by the Company – and is used for business purposes (even if also used for personal purposes) or is used in connection with CI (even if it also stores private data). Any Personal Device that is not used for business purposes and is not used in conjunction with CI is out of scope of this policy and is an Exempt Personal Device.
Personal Information or Personally Identifiable Information (PII):	Any information which uniquely identifies an individual that can be used on its own or in combination with other information to identify contacts or locate a person (e.g., directly or indirectly in particular by reference to an identification number or to one or more factors specific to a physical, physiological, mental, economic, cultural or social identity). Sensitive personal information includes PII that could be used to commit identity theft, such as Social Security numbers, driver's license numbers, and financial account numbers.
Personnel	Includes all employees, temporary employees, contractors, sub-contractors, and their respective facilities supporting Company business operations, wherever CI is stored or processed, including any third party contracted by the Company to handle, process, transmit, store, or dispose of CI.
Policy	A formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.
Port Scanning	The act of probing a system to identify open ports.
Procedure	An established or official way of doing something, based on a series of actions conducted in a certain order of manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.
Proprietary Information	Information unique to a company and its ability to compete, including, but not limited to; customer lists, technical data, product costs, and trade secrets.
Purge	Rendering sanitized data unrecoverable by laboratory attack methods.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (e.g., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote access	Access to a company information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). Remote access methods include, for example, dial-up,

	broadband, and wireless. Virtual Privacy Networks (VPNs), when adequately provisioned with appropriate security controls, are considered internal networks
Removable Data Storage Media	Disks, Tapes, DVDs, CDs, USB Thumb Drives, external hard drives, and other data storage devices purchased, provided or approved by the Company for business use by users, or otherwise used in connection with CI.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: • The adverse impacts that would arise if the circumstance or event occurs; and • The likelihood of occurrence.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and includes: • Establishing the context for risk-related activities; • Assessing risk; • Responding to risk once determined; and • Monitoring risk over time.
Role-Based Access Control (RBAC)	Access control based on user roles.
Safeguards	Protective measures prescribed to meet the security requirements (e.g., confidentiality, integrity, and availability) specified for an information system.
Sanitization:	Sanitization: Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. A process of removing information from media, such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the Company's risk management approach.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Control Assessment	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security Domain	A domain that implements a security policy and is administered by a single authority.

Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis	Security Impact Analysis: The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Requirement	A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. **Note:** Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.
Sensitive information	Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled. A term that covers categories of information that must be kept safeguarded. Examples of Sensitive Information include PII, Non-public Personal Information (NPI), and all other forms of data classified as LD Restricted or LD Confidential.
Social Media	Internet-based tools and services that allow subscribers to network and communicate with each other as well as share data, photos, files, and other user generated content, or to provide updates about themselves, as well as other sites that allow users to read and share their views, or virtual worlds, to name some of the more common social media segments. Some popular social media services include, but are not limited to, Facebook, LinkedIn, Twitter, and YouTube, as well as blogs, vlogs, and content sharing sites.
Software	Any application installed by the Company on Company Equipment, including but not limited to: • Desktop computers • Mobile Devices
Standard	Formally established requirements in regard to processes, actions, and configurations.
Subject	An individual, process, or device causing information to flow among objects or change to the system state.
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begin with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Teleworking	A work arrangement that allows a user to perform work, during any part of regular, paid hours, at an approved alternative worksite (e.g. home or telework center).
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals or other organizations through an information system via unauthorized access, destruction, disclosure, and/or modification of information.
Usenet Newsgroup	A repository for messages posted from many users in different locations.

Virtual Privacy Network (VPN)	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.